

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application: 1999年 5月31日

出 願 番 号

Application Number: 平成11年特許願第152060号

出 願 人

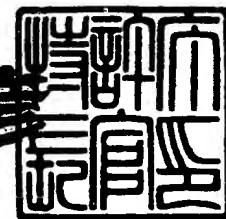
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 4月14日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3025977

【書類名】 特許願

【整理番号】 9900443003

【提出日】 平成11年 5月31日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 石黒 隆二

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 岡上 拓巳

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 大石 丈於

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100082131

 【弁理士】

 【氏名又は名称】 稲本 義雄

 【電話番号】 03-3369-6479

【手数料の表示】

 【予納台帳番号】 032089

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、並びに媒体

【特許請求の範囲】

【請求項 1】 暗号鍵で暗号化されているデータを蓄積する蓄積手段と、
前記蓄積手段により蓄積されたデータの管理情報を保持する保持手段と、
前記管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報
と、前記暗号鍵に基づき所定の演算を行う演算手段と、
前記演算手段の演算結果を記憶する記憶手段と、
前記演算手段の演算結果と、前記記憶手段に記憶されている過去の前記演算結
果とを比較し、比較結果に対応して前記蓄積手段に蓄積されている前記データの
利用を制御する制御手段と
を備えることを特徴とする情報処理装置。

【請求項 2】 前記演算手段は、前記演算情報と前記暗号鍵にハッシュ関数
を適用して前記演算を行う
ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記データは音楽データであり、
前記演算情報は、前記音楽データを識別する識別情報を含み、
前記保持手段は、通常、読み出しまたは書き込みを行うことができない領域に
前記更新情報を保持する
ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 暗号鍵で暗号化されているデータを蓄積する蓄積ステップと、
前記蓄積ステップの処理により蓄積されたデータの管理情報を保持する保持ス
テップと、
前記管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報
を、前記暗号鍵に基づき所定の演算を行う演算ステップと、
前記演算ステップの演算結果を記憶する記憶ステップと、
前記演算ステップの演算結果と、前記記憶ステップの処理で記憶された過去の
前記演算結果とを比較し、比較結果に対応して前記蓄積ステップの処理で蓄積さ

れた前記データの利用を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項 5】 暗号鍵で暗号化されているデータを蓄積する蓄積ステップと

前記蓄積ステップの処理により蓄積されたデータの管理情報を保持する保持ステップと、

前記管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報を、前記暗号鍵に基づき所定の演算を行う演算ステップと、

前記演算ステップの演算結果を記憶する記憶ステップと、

前記演算ステップの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果とを比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップと

を含むことを特徴とするプログラムをコンピュータに実行させる媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びに媒体に関し、特に、改竄を防止し、不正な複製を抑制することができるようにした、情報処理装置および方法、並びに媒体に関する。

【0002】

【従来の技術】

最近、デジタル技術の普及にともない、音楽データ、画像データなどの各種のデータがデジタル的に記録媒体に記録または再生されるようになってきた。その結果、複数回コピーしても、画質あるいは音質が劣化しないデータを得ることが可能となってきた。

【0003】

【発明が解決しようとする課題】

しかしながら、このようにデジタル技術が発達してくると、次のような問題が発生する。

【0004】

(1) 例えば、コンパクトディスク(CD)からパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、CDからの音楽データが、そのまま、あるいは圧縮符号化されてハードディスクに記録されるので、例えば、インターネットなどのネットワークを介して複製を違法に大量に配布することができてしまう。

【0005】

(2) CDからパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、そのコピー回数に制限がないため、複製が大量に配布されてしまう。

【0006】

(3) パーソナルコンピュータのハードディスク内のデジタル音楽データを、例えば、メモリスティックウォークマン(商標)などの外部の機器に移す場合、移した後もハードディスク内に元のデジタル音楽データが残るので、複製が大量に配布できてしまう恐れがある。

【0007】

(4) 上記した(3)の問題を防止するために、デジタル音楽データを外部の機器に移した後に、データの送り元としてのハードディスクのデータを消去するように(いわゆる、音楽データをムーブするように)パーソナルコンピュータのソフトウェアを作成しておけばよいが、例えば、ムーブの前にハードディスクの内容を別の記録媒体へバックアップしておき、ムーブの後に、バックアップしたデータをハードディスクにリストアすれば、結局、ムーブしたはずのデータがハードディスクに残ってしまうことになる。

【0008】

(5) パーソナルコンピュータが、ハードディスク内のデジタル音楽データをメモリスティックウォークマンなどの外部の機器に移す場合、外部機器がどのような機器であるかを確認しないため、違法な機器にデジタル音楽データが渡されてしまう恐れがある。

【0009】

(6) メモリスティックウォークマンなどの外部の機器から、パーソナルコンピュータにデジタル音楽データを渡す場合、そのパーソナルコンピュータを制御しているソフトウェアがどのようなソフトウェアであるかを確認しないため、違法なソフトウェアに対してデジタル音楽データが渡されてしまう恐れがある。

【0 0 1 0】

(7) CDより再生された音楽データをパーソナルコンピュータで取り扱うとき、複数の曲が同一か否かを判断するために、曲データに含まれるISRC(International Standard Recording Code)を使用することが可能であるが、CDによっては、ISRCデータを含んでいないものがある。この場合、複数の曲が同一であるか否かを判定することができなくなる。

【0 0 1 1】

(8) 以上のような各機能は、パーソナルコンピュータ上で、ソフトウェアの制御により実現されるため、そのソフトウェアが改竄されると、システムの作成者が意図しない動作を行わせることができてしまう。

【0 0 1 2】

本発明はこのような状況に鑑みてなされたものであり、記録媒体に蓄積されているデータが改竄され、不正に利用されるのを防止することができるようにするものである。

【0 0 1 3】

【課題を解決するための手段】

請求項 1 に記載の情報処理装置は、暗号鍵で暗号化されているデータを蓄積する蓄積手段と、蓄積手段により蓄積されたデータの管理情報を保持する保持手段と、管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報と、暗号鍵に基づき所定の演算を行う演算手段と、演算手段の演算結果を記憶する記憶手段と、演算手段の演算結果と、記憶手段に記憶されている過去の演算結果とを比較し、比較結果に対応して蓄積手段に蓄積されているデータの利用を制御する制御手段とを備えることを特徴とする。

【0 0 1 4】

請求項 4 に記載の情報処理方法は、暗号鍵で暗号化されているデータを蓄積す

る蓄積ステップと、蓄積ステップの処理により蓄積されたデータの管理情報を保持する保持ステップと、管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報を、暗号鍵に基づき所定の演算を行う演算ステップと、演算ステップの演算結果を記憶する記憶ステップと、演算ステップの演算結果と、記憶ステップの処理で記憶された過去の演算結果とを比較し、比較結果に対応して蓄積ステップの処理で蓄積されたデータの利用を制御する制御ステップとを含むことを特徴とする。

【0015】

請求項5に記載の媒体のプログラムは、暗号鍵で暗号化されているデータを蓄積する蓄積ステップと、蓄積ステップの処理により蓄積されたデータの管理情報を保持する保持ステップと、管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報を、暗号鍵に基づき所定の演算を行う演算ステップと、演算ステップの演算結果を記憶する記憶ステップと、演算ステップの演算結果と、記憶ステップの処理で記憶された過去の演算結果とを比較し、比較結果に対応して蓄積ステップの処理で蓄積されたデータの利用を制御する制御ステップとを含むことを特徴とする。

【0016】

請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載の媒体においては、演算情報と暗号鍵に基づき所定の演算が行われ、その演算結果と、過去の演算結果とが比較され、その比較結果に対応して、蓄積されているデータの利用が制御される。

【0017】

【発明の実施の形態】

図1は、本発明を適用したネットワークシステムの構成例を表している。パーソナルコンピュータ1は、各種の処理を実行するCPU (Central Processing Unit) 12、各種のプログラムやデータを一時的に記憶するメモリ13、並びに、各種のプログラムやデータを大量に蓄積するハードディスク15を備えている。CD-ROM (Read Only Memory) ドライブ14は、装着されたCD-ROMに記録されているプログラムやデータを読み出す。IEC (International Electrotechnical Commis

sion) 6 0 9 5 8 端子 1 6 a を有する音声入出力インタフェース 1 6 は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。インターネット接続インタフェース 1 1 は、インターネット 4 との間のインタフェース処理を実行する。インタフェース 1 7 は、アダプタ 7 またはメモリスティックウォークマン 6 との間のインタフェース処理、並びに、入力部 2 およびディスプレイ 3 に対するインタフェース処理を実行する。

【 0 0 1 8 】

半導体 IC として、一体的に形成され、パーソナルコンピュータ 1 に装着されるアダプタ 7 の CPU 3 2 は、インタフェース 3 1 を介してパーソナルコンピュータ 1 の CPU 1 2 と共働し、各種の処理を実行する。RAM(Random Access Memory) 3 3 は、CPU 3 2 が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ 3 4 は、パーソナルコンピュータ 1 の電源がオフされた後も保持する必要があるデータを記憶する。ROM 3 6 には、パーソナルコンピュータ 1 から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) 3 5 は、計時動作を実行し、時刻情報を提供する。

【 0 0 1 9 】

メモリスティックウォークマン 6 は、不揮発性メモリ（メモリスティック（商標））2 3 を有し、パーソナルコンピュータ 1 からインタフェース 2 1 と制御部 2 2 を介して提供されたデジタル音楽データを記憶する。制御部 2 2 は、パーソナルコンピュータ 1 と不揮発性メモリ 2 3 との間でデータを授受するとき、相互に認証処理を実行する。インタフェース 2 1 は、パーソナルコンピュータ 1 との間のインタフェース処理、あるいは不揮発性メモリ 2 3 に記憶されている音楽データを読み出し、ヘッドホンなどを介してユーザに提供するためのインタフェース処理を実行する。

【 0 0 2 0 】

パーソナルコンピュータ 1 は、インターネット 4 を介して EMD (Electrical Music Distribution) サーバ 5 と接続されており、EMD サーバ 5 から音楽データの提供を受けることができる。

【 0 0 2 1 】

次に、メモリスティックウォークマン 6 の不揮発性メモリ 2 3 に記憶されている音楽データの不正コピーを防止する方法について説明する。

【 0 0 2 2 】

メモリスティックウォークマン 6 の不揮発性メモリ 2 3 に記憶されている曲ファイルは、図 2 に示すように、ヘッダ部とデータ部に区分されており、ヘッダ部には、曲識別子 (ID)、再生回数、再生期限、曲名、およびアーティスト名などの情報が記憶され、データ部には、暗号化された音楽データなどが記述されている。この例においては、データの改竄を防止するために、曲ファイルのヘッダ部に、MAC (Message Authentication Code) 値が記録される。MAC は、keyed hash といわれる鍵付き一方向性関数 (例えば、SHA、DES 等が用いられる) により、式 (1) に示すように演算される。

【 0 0 2 3 】

$$\text{MAC 値} = \text{MAC} (K_c, \text{重要情報}) \quad \dots (1)$$

ここで、 K_c は、データ部に記録されているデータを暗号化しているコンテンツ鍵 (暗号鍵) である。また、重要情報は、ヘッダ部に記憶されている情報のうちの所定のもの (例えば、曲識別子、再生回数、および再生期限) である。

【 0 0 2 4 】

図 3 は、このようなメモリスティックウォークマン 6 の不揮発性メモリ 2 3 に記録されているデータをパーソナルコンピュータ 1 により再生する場合の処理を表わしている。ステップ S 1 において、パーソナルコンピュータ 1 の CPU 1 2、あるいは CPU 1 2 上で動作するアプリケーション (以下の説明では、CPU 1 2 とする) は、メモリスティックウォークマン 6 の制御部 2 2 と相互認証処理を行い、通信用鍵 K_s を共有し、それを利用して、さらに不揮発性メモリ 2 3 のデータ部に記憶されているデータを暗号化している暗号鍵 K_c を取得する。

【 0 0 2 5 】

すなわち、CPU 1 2 は、制御部 2 2 と相互認証処理を実行し、通信用鍵 K_{s1} を共有する。制御部 2 2 は、また、不揮発性メモリ 2 3 と相互認証処理を実行し、

通信用鍵 K_{s_2} を共有する。

【0026】

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、不揮発性メモリ 23 は、内部に記憶している暗号鍵 K_c （保存用鍵で暗号化されている）を、やはり内部に記憶している保存用鍵で復号し、通信用鍵 K_{s_2} で暗号化して、制御部 22 に転送する。制御部 22 は、転送を受けた暗号鍵 K_c を通信用鍵 K_{s_2} で復号する。

【0027】

また、このとき、不揮発性メモリ 23 は、曲ファイルのヘッダ部に記憶されている重要情報と前回の MAC 値を読み出し、通信用鍵 K_{s_2} で暗号化して制御部 22 に転送する。制御部 22 は、これを受信すると、通信用鍵 K_{s_2} で復号する。

【0028】

制御部 22 は、暗号鍵 K_c 、重要情報、および前回の MAC 値を、通信用鍵 K_{s_1} で暗号化し、CPU 12 に転送する。CPU 12 は、これを通信用鍵 K_{s_1} で復号する。

【0029】

このように、不揮発性メモリ 23 と制御部 22 の間、または、制御部 22 と CPU 12（アプリケーション）との間には、それぞれ通信用鍵 K_{s_2} 、または通信用鍵 K_{s_1} で暗号化して、データが授受されるが、以下の説明においては、この暗号化処理の説明は、特に強調する必要がある場合を除き、省略する。

【0030】

ステップ S2 において、CPU 12 は、ステップ S1 で取得した暗号鍵 K_c と、曲ファイルのヘッダ部の重要情報とから、上記した式（1）に従って、MAC 値を演算し、その値を R に設定する。ステップ S3 において、CPU 12 は、ステップ S2 で演算された値 R と、前回演算され、曲ファイルのヘッダ部に保存されていた MAC 値とを比較する。両者が一致しない場合、CPU 12 は、ステップ S4 に進み、例えば、「曲ファイルが改竄された恐れがあります」のようなメッセージを、ディスプレイ 3 に表示させた後、処理を終了させる。この場合においては、メモリスティックウォークマン 6 の不揮発性メモリ 23 に記録されている音楽データ

は、改竄されたものであり、再生が実行されない。

【0031】

値Rと曲ファイルのヘッダ部に保存しておいたMAC値が一致すると判定された場合、ステップS5に進み、CPU12は、制御部22を介して、不揮発性メモリ23から、暗号化されている音楽データの転送を受け、それを暗号鍵Kcで復号し、音声入出力インタフェース16を介して出力（再生）する。

【0032】

ステップS6において、CPU12は、制御部22を制御し、不揮発性メモリ23の曲ファイルのヘッダ部の重要情報の中の再生回数の値を1だけインクリメントさせる。さらに、CPU12は、ステップS7において、制御部22を制御し、新たな重要情報（その再生回数の値が1だけインクリメントされている）を用いて、式（1）に従って、MAC値を演算させ、そのMAC値で、不揮発性メモリ23の曲ファイルのヘッダ部に保存されているMAC値を更新させる。MAC値は、暗号鍵Kcがないと演算できないため、認証を受けた機器あるいはアプリケーションだけが、演算できることになる。

【0033】

しかしながら、図3の方法は、図4に示した方法による不正を防止することができない。すなわち、まず、最初に不揮発性メモリ23-1の曲ファイル（そのMAC値として、MAC1が記録されているものとする）がハードディスク15にバックアップされたとすると、これがハードディスク15に、曲ファイル1（MAC1）として記憶される。このとき、不揮発性メモリ23-1には、オリジナルの曲ファイル（MAC1）が残る。

【0034】

次に、不揮発性メモリ23-1の曲ファイル（MAC1）がハードディスク15に移動されると、これが、ハードディスク15に、曲ファイル2（MAC1）として記憶される。このとき、不揮発性メモリ23-1の曲ファイル（MAC1）は削除され、ハードディスク15には、曲ファイル1（MAC1）と曲ファイル2（MAC1）の2つの曲ファイルが記憶される。

【0035】

さらに、ハードディスク 1 5 の曲ファイル 1 (MAC 1) が不揮発性メモリ 2 3 - 1 にリストアされると、ハードディスク 1 5 には曲ファイル 2 (MAC 1) が残る。ハードディスク 1 5 の曲ファイル 2 (MAC 1) が他の不揮発性メモリ 2 3 - 2 に移動されると、結果的に、同一の曲ファイル (MAC 1) が 2 つの不揮発性メモリ 2 3 - 1, 2 3 - 2 に記憶されたことになる。従って、不揮発性メモリ 2 3 - 2 に記憶された曲ファイル 2 (MAC 1) を、不揮発性メモリ 2 3 - 1 に記憶された曲ファイル 1 (MAC 1) と同様に再生することができる。

【 0 0 3 6 】

このような不正を防止するために、例えば、MAC 値を、次式 (2) で示すようにして求めることができる。式 (2) において、変数 seq# は、コピーや移動が行われる毎に更新 (例えばインクリメント) される変数であり、不揮発性メモリ 2 3 の、通常のアプリケーションによるアクセスが禁止されている (アダプタ 7 または認証を受けたアプリケーションのみがアクセス可能な) media defect list (メディア ディフェクト リスト) の 0 番目の block に記憶される。また、|| は連結 (または結合) を意味し、A || B は、データ A (a ビット) の最下位ビット (LSB (Least Significant Bit)) 側にデータ B (b ビット) を単純に結合して、a + b ビットにしたデータを意味する。

【 0 0 3 7 】

MAC 値 = MAC (K c , seq# || 重要情報) . . . (2)

media defect list は、図 5 (A) に示すように、defect (bad) block (欠陥を有するブロック) と、その交代ブロックを登録しておくリストで、基本的に、ここに defect block として登録されると、その block に対する読み出しおよび書き込みは禁止され、その代わりに、交代ブロックに対して読み出しおよび書き込みが行われる。ただし、0 番目の defect block には、欠陥を有しない block が登録されており、制御部 2 2 は、特別なコマンドを受信したときにだけ、そこに対する読み出しおよび書き込みを実行するようになされている。変数 seq# は、図 5 (B) に示すように、この 0 番目の defect block に記憶される。

【 0 0 3 8 】

この特別な指令 (コマンド) を出すことができるのは、アダプタ 7 と認証を受

けたアプリケーションだけとされる。従って、0番目のdefect blockにアクセスすることができるのは、アダプタ7と認証を受けたアプリケーションだけとなる。

【0039】

変数seq#は、それぞれの曲（トラック）に対して、一対一に割り振られているため、MAC値の再演算は、その各曲（トラック）毎に行われる。

【0040】

なお、変数seq#を記憶する領域は、media defect listの0番目のdefect blockに限られるものではなく、一般的に、読み出しおよび書き込みが禁止される領域であれば、それらを利用しても良い。

【0041】

図6は、このような不揮発性メモリ23に記録されている曲ファイルをハードディスク15に移動する場合の処理を表わしている。

【0042】

ステップS21において、制御部22は、メモリスティック（不揮発性メモリ23）と認証し、暗号鍵Kcを取得する。ステップS22において、パーソナルコンピュータ1のCPU12、あるいはパーソナルコンピュータ1に搭載されているアプリケーション（以下の説明では、アプリケーションとする）は、メモリスティックウォークマン6（制御部22）と相互認証処理を行い、通信用鍵Ksを共有する。この処理は、上述した図3のステップS1の処理と同様の処理である（但し、ステップS1では、このとき共有する通信用鍵をKs₁としている）。

【0043】

ステップS23において、アプリケーション（認証されている）は、制御部22に特別なコマンドを出力し、不揮発性メモリ23のmedia defect listの0番目のdefect blockに記憶されている変数seq#を、所定の値に更新させる。

【0044】

ステップS24において、制御部22は、ステップS21で不揮発性メモリ23から取得した暗号鍵Kcを、ステップS22との間で取得した通信用鍵Ksで暗号化し、アプリケーションへ転送する。ステップS25において、制御部22

は、不揮発性メモリ 23 に記憶されている曲ファイルのデータ部の、暗号化されている音楽データの転送を受け、通信用鍵 K_s で暗号化して、アプリケーションへ転送し、ハードディスク 15 にコピーさせる。ステップ S 26 において、アプリケーションは、メモリスティックウォークマン 6 から転送されてきた暗号鍵 K_c を通信用鍵 K_s で復号し、自分自身の保存用鍵で暗号化し、ハードディスク 15 に記憶する。

【0045】

ステップ S 27 において、アプリケーションは、制御部 22 に対して、音楽データがコピーされたことを通知する。このとき制御部 22 は、ステップ S 28 において、不揮発性メモリ 23 に記憶されている曲ファイル（ステップ S 25 で、アプリケーションに転送した曲ファイル）を削除する。

【0046】

移動処理をこのように行うようにすると、図 4 を参照して説明した不正コピーを防止することができる。いま、例えば、図 7 に示すように、不揮発性メモリ 23-1 に曲 A が記録されているものとする。この場合、曲 A の重要情報に対応する MAC 値としての MAC 1 が曲 A のヘッダ部に保存され、変数 seq 1 が、media defect list の 0 番目の defect block に、曲 A に対応して記憶されている（以下、この場合の状態を、“A (MAC 1), seq 1” のように記述する）。この状態において、記録データ（曲ファイル）をハードディスク 15 にバックアップしたとする。このとき、ハードディスク 15 には曲 A (MAC 1) が記憶されているが、不揮発性メモリ 23 の変数 seq 1 と MAC 1 は更新されていないので、不揮発性メモリ 23-1 には、曲 A (MAC 1), seq 1 が残る。

【0047】

次に、不揮発性メモリ 23-1 の曲 A (MAC 1), seq 1 をハードディスク 15 に移動させた場合、その時点において、不揮発性メモリ 23-1 の変数 seq 1 は、変数 seq 2 に更新される（ステップ S 23）が、MAC 1 は更新されていないので、ハードディスク 15 には、曲 A (MAC 1) が、新たに記録される。制御部 22 は、アプリケーションからの通知（曲 A が移動された旨の通知）を受け、不揮発性メモリ 23-1 に記録されている曲 A を削除させる。

【 0 0 4 8 】

その後、ハードディスク 1 5 にバックアップされた曲 A (MAC 1) を不揮発性メモリ 2 3 - 1 にリストアすると、不揮発性メモリ 2 3 - 1 には、曲 A (MAC 1) , seq 2 が保存される。さらに、ハードディスク 1 5 に移動された曲 A (MAC 1) を他の不揮発性メモリ 2 3 - 2 に移動させると、変数 seq 2 が、さらに変数 seq 3 に更新され、記録される曲は、曲 A (MAC 1) , seq 3 となる。

【 0 0 4 9 】

この不揮発性メモリ 2 3 - 1 または 2 3 - 2 が、図 3 のフローチャートに沿って再生されると、ステップ S 2 の処理で MAC 値の演算には、変数 seq 2 (または seq 3) が用いられることになり、変数 seq 1 を用いて演算され、曲ファイルのヘッダ部に記憶されている MAC 1 とは異なる値となる。その結果、ステップ S 3 で判定が NO になり、この曲は不正にコピーされたとして、再生されることはない。

【 0 0 5 0 】

以上においては、記録媒体として、メモリスティックウォークマン 6 の不揮発性メモリ (メモリスティック) 2 3 を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。

【 0 0 5 1 】

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

【 0 0 5 2 】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアとしてのメモリスティックウォークマン 6 に組み込まれているコンピュータ (制御部 2 2 に対応する)、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどにインストールされる。

【 0 0 5 3 】

次に、図 8 を参照して、上述した一連の処理を実行するプログラムをコンピュータにインストールし、コンピュータによって実行可能な状態とするために用いられる媒体について、そのコンピュータが汎用のパーソナルコンピュータである場合を例として説明する。

【0054】

プログラムは、図 8 (A) に示すように、パーソナルコンピュータ 51 に内蔵されている記録媒体としてのハードディスク 52 (図 1 のパーソナルコンピュータ 1 に内蔵されているハードディスク 15 に対応する) や半導体メモリ 53 に予めインストールした状態でユーザに提供することができる。

【0055】

あるいはまた、プログラムは、図 8 (B) に示すように、フロッピーディスク 61、CD-ROM 62、MO (Magneto-Optical) ディスク 63、DVD (Digital Versatile Disk) 64、磁気ディスク 65、または半導体メモリ 66 などの記録媒体に、一時的あるいは永続的に格納し、パッケージソフトウェアとして提供することができる。

【0056】

さらに、プログラムは、図 8 (C) に示すように、ダウンロードサイト 71 から、デジタル衛星放送用の人工衛星 72 を介して、パーソナルコンピュータ 51 に無線で転送したり、ローカルエリアネットワーク、インターネットといったネットワーク 81 を介して、パーソナルコンピュータ 51 に有線で転送し、パーソナルコンピュータ 51 おいて、内蔵するハードディスク 52 などに格納させることができる。

【0057】

本明細書における媒体とは、これら全ての媒体を含む広義の概念を意味するものである。

【0058】

パーソナルコンピュータ 51 は、例えば、図 9 に示すように、CPU 92 を内蔵している。CPU 92 にはバス 91 を介して入出力インタフェース 95 が接続されており、CPU 92 は、入出力インタフェース 95 を介して、ユーザから、キーボ

ード、マウスなどよりなる入力部 9 7 から指令が入力されると、それに対応して、図 8 (A) の半導体メモリ 5 3 に対応する ROM 9 3 に格納されているプログラムを実行する。あるいはまた、CPU 9 2 は、ハードディスク 5 2 に予め格納されているプログラム、人工衛星 7 2 もしくはネットワーク 8 1 から転送され、通信部 9 8 により受信され、さらにハードディスク 5 2 にインストールされたプログラム、またはドライブ 9 9 に装着されたフロッピーディスク 6 1、CD-ROM 6 2、MO ディスク 6 3、DVD 6 4、もしくは磁気ディスク 6 5 から読み出され、ハードディスク 5 2 にインストールされたプログラムを、RAM 9 4 にロードして実行する。さらに、CPU 9 2 は、その処理結果を、例えば、入出力インタフェース 9 5 を介して、LCD (Liquid Crystal Display) などよりなる表示部 9 6 に必要に応じて出力する。

【0059】

なお、本明細書において、媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0060】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0061】

【発明の効果】

請求項 1 に記載の情報処理装置、請求項 4 に記載の情報処理方法、および請求項 5 に記載の媒体によれば、演算情報と暗号鍵に基づき所定の演算を行い、その演算結果と、過去の演算結果とを比較し、その比較結果に対応して、蓄積されているデータの利用を制御するようにしたので、改竄が行われたとしても、それを検出することができ、蓄積されているデータの不正な複製を防止することが可能となる。

【図面の簡単な説明】

【図 1】

本発明を適用したシステムの構成例を示すブロック図である。

【図 2】

曲ファイルを説明する図である。

【図 3】

図 1 のメモリスティックウォークマン 6 からパーソナルコンピュータ 1 にデータを出力する場合の処理を説明するフローチャートである。

【図 4】

図 3 の処理に関する不揮発性メモリ 2 3 の動作を説明する図である。

【図 5】

media defect list を説明する図である。

【図 6】

図 1 のメモリスティックウォークマン 6 からハードディスク 1 5 へデータを移動する場合の処理を説明するフローチャートである。

【図 7】

図 6 の処理に関する不揮発性メモリ 2 3 の動作を説明する図である。

【図 8】

媒体を説明する図である。

【図 9】

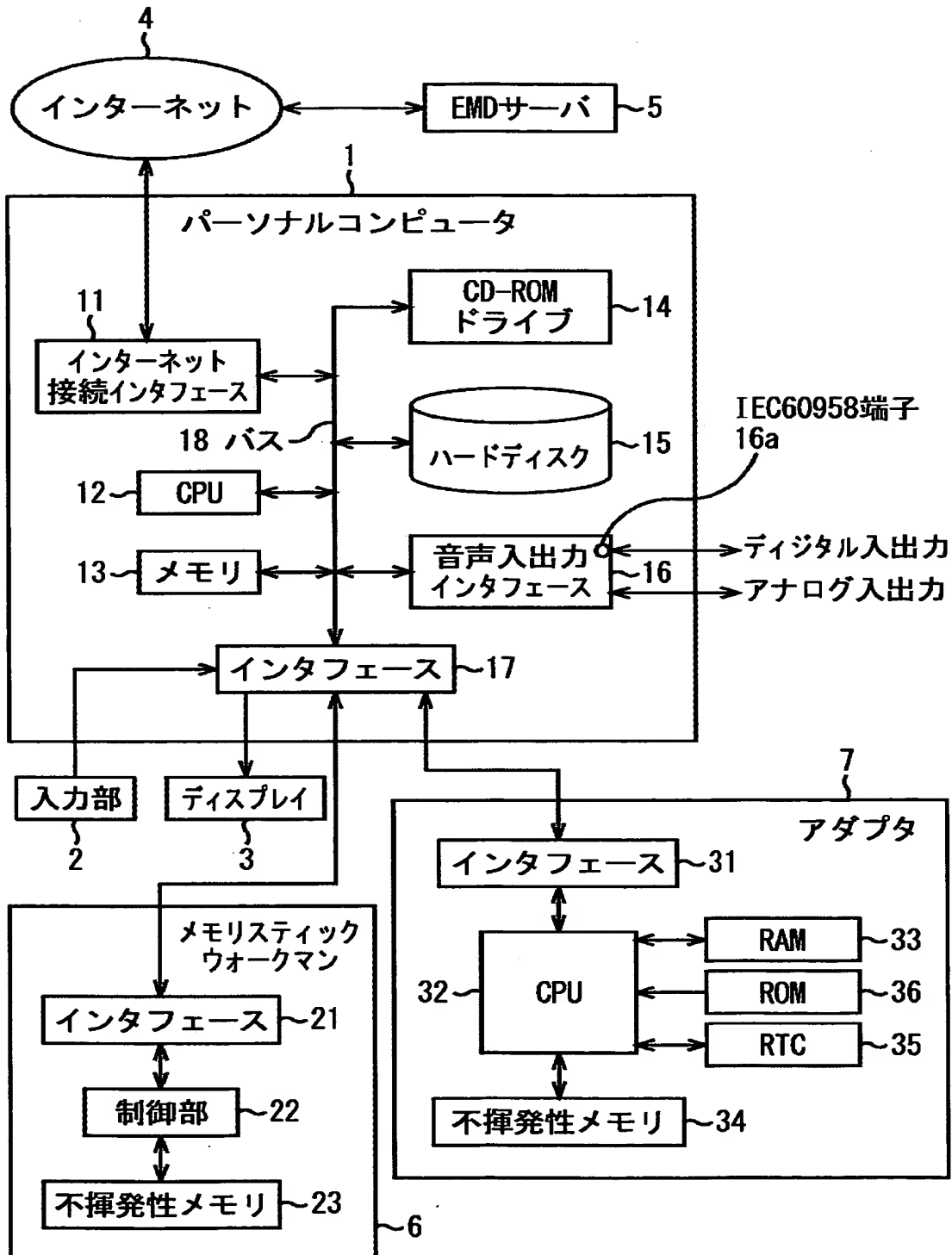
図 8 のパーソナルコンピュータ 5 1 の構成を示すブロック図である。

【符号の説明】

1 パーソナルコンピュータ, 2 入力部, 3 ディスプレイ, 4 インターネット, 5 EMDサーバ, 6 メモリスティックウォークマン, 7 アダプタ, 12 CPU, 13 メモリ, 14 CD-ROMドライブ, 15 ハードディスク, 16 音声入出力インタフェース, 16a IEC60958端子, 22 制御部, 23-1, 23-2 不揮発性メモリ, 32 CPU

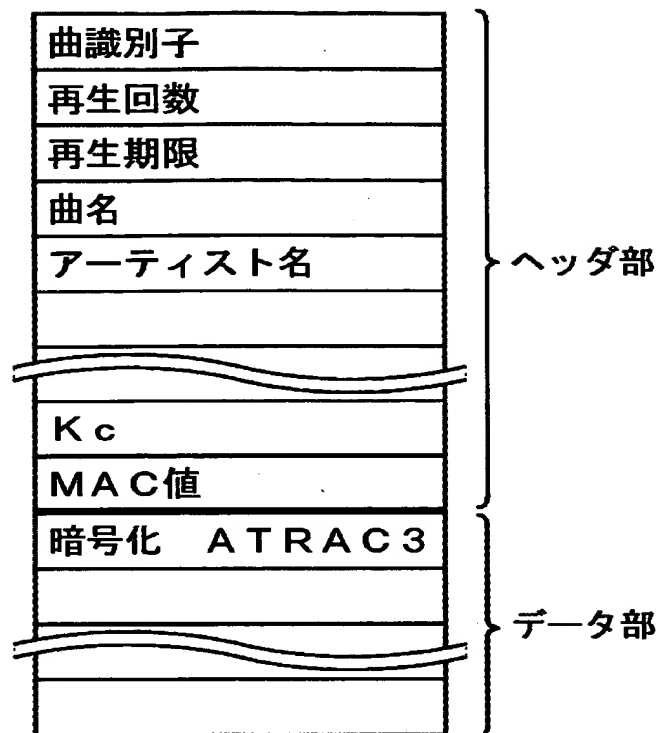
【書類名】 図面

【図 1】

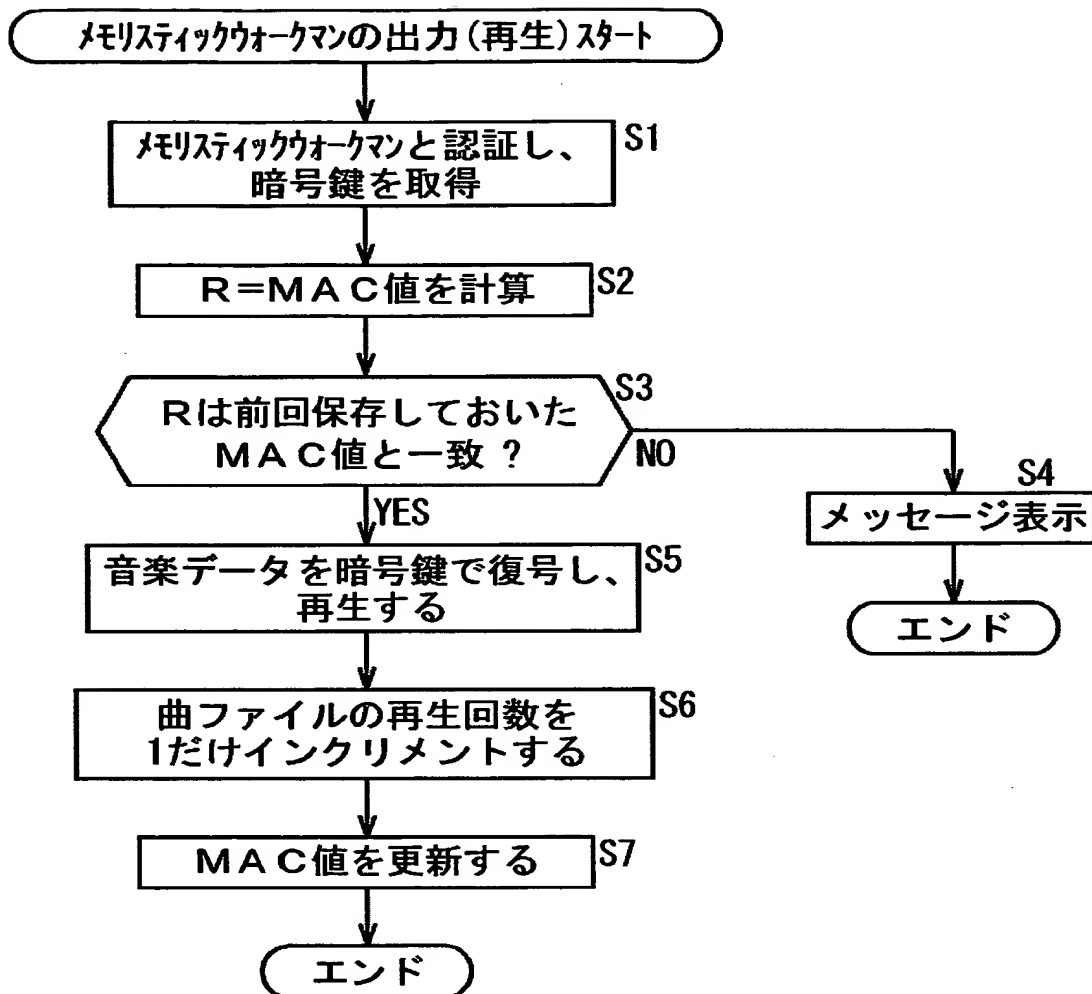


【図 2】

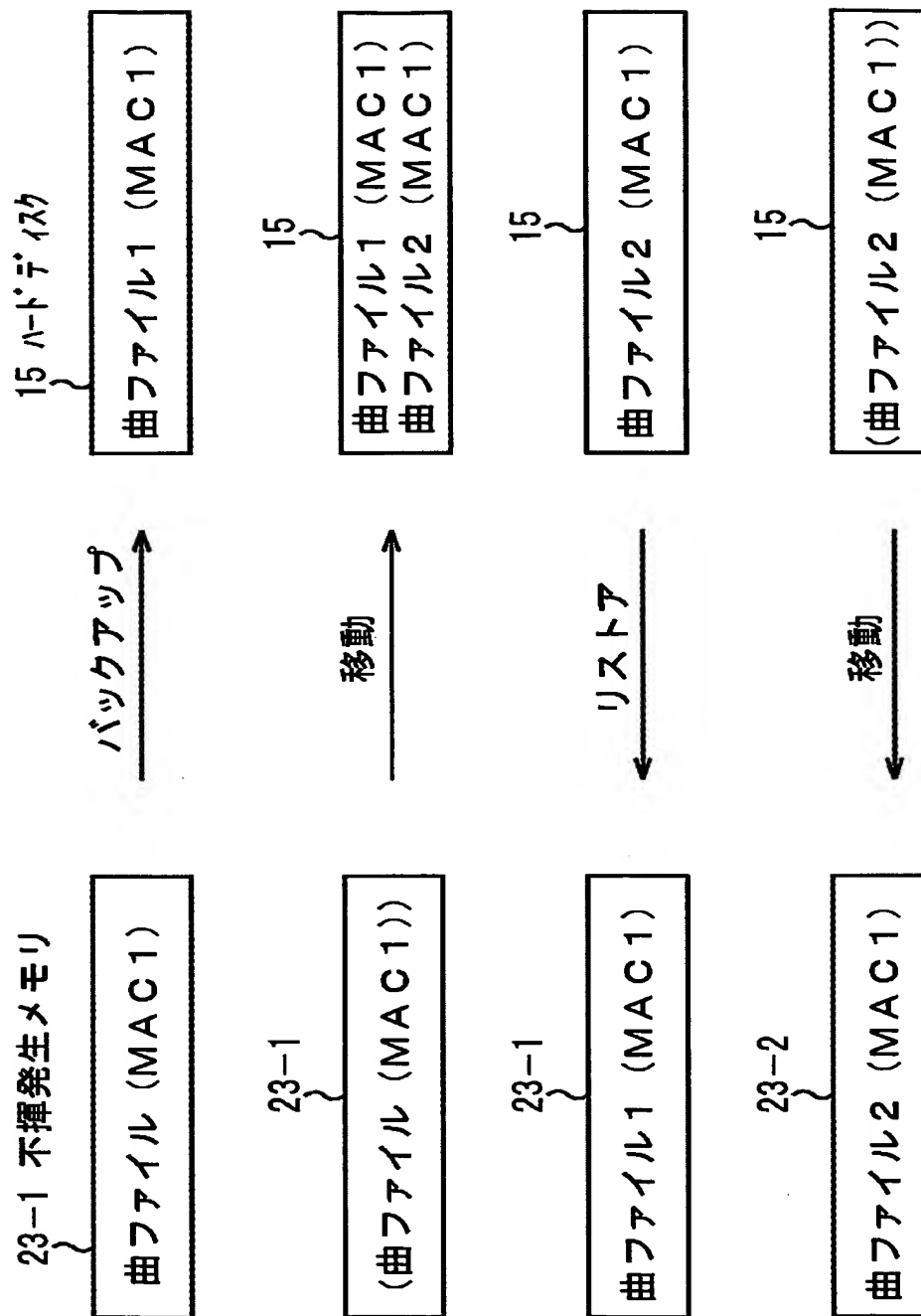
曲ファイル



【図 3】



【図 4】



【図 5】

(A)

Media defect list

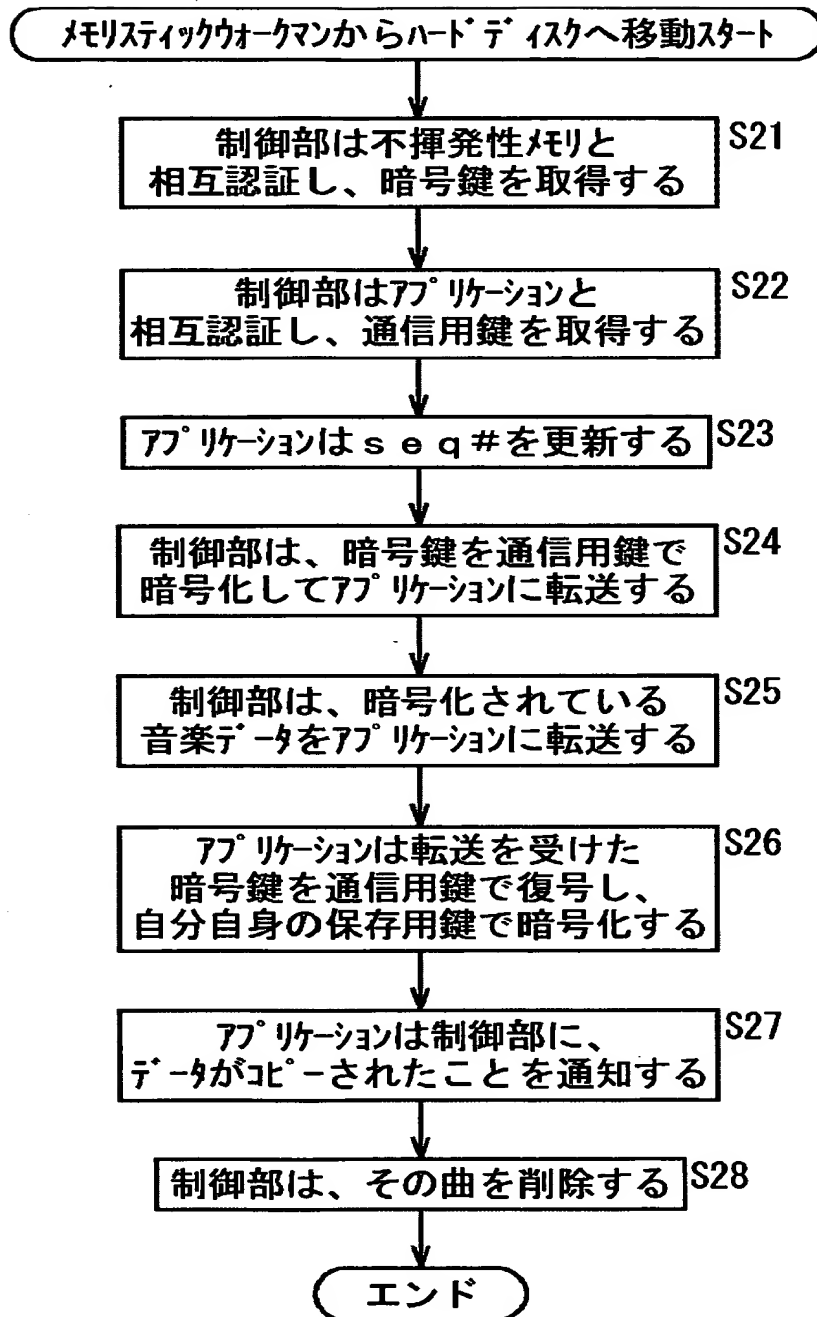
	defect (bad) block	交代ブロック
0		
1		
2		
3		
4		
5		

(B)

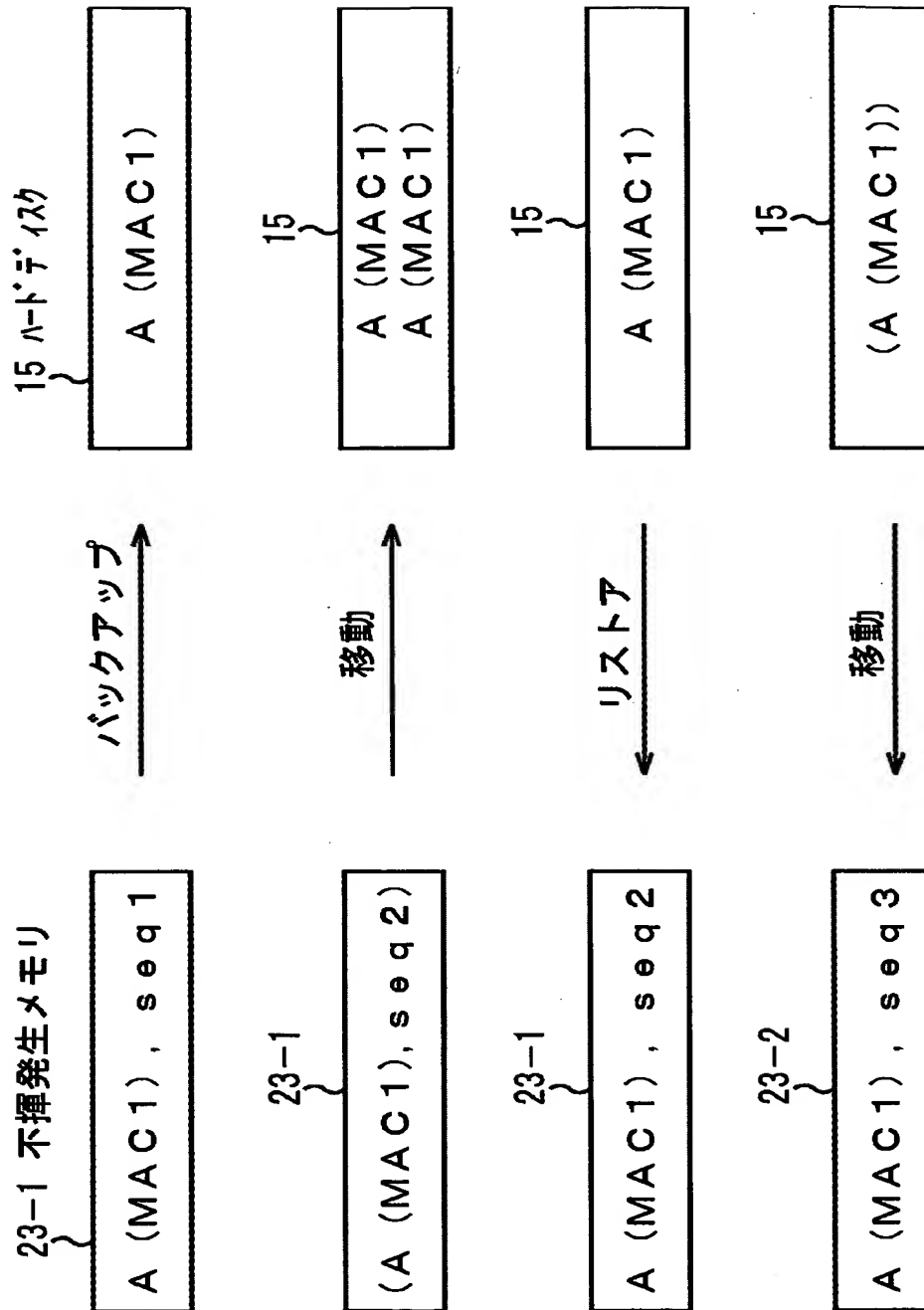
0番目defect block

s e q 1
s e q 2
s e q 3
s e q 4

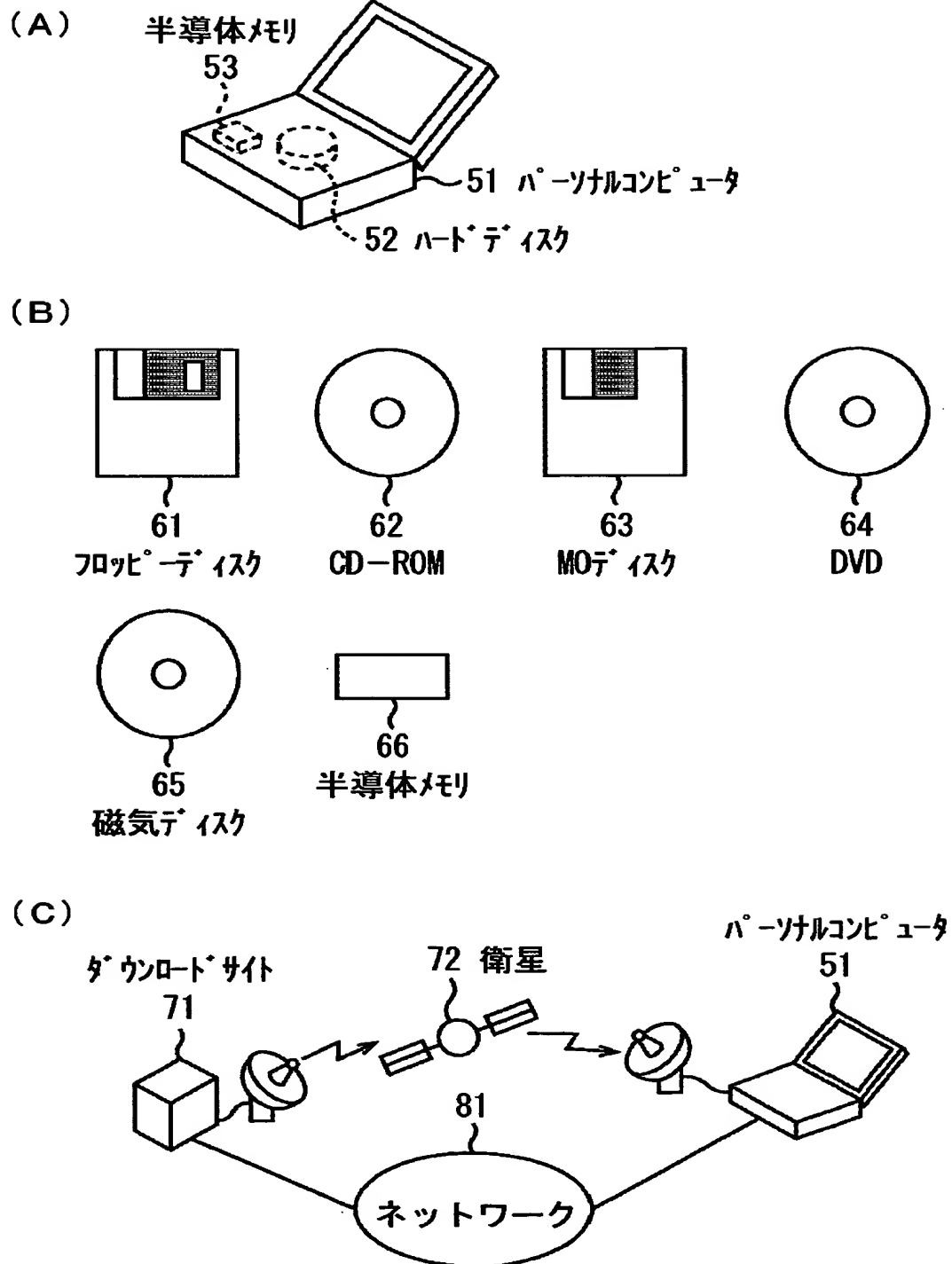
【図 6】



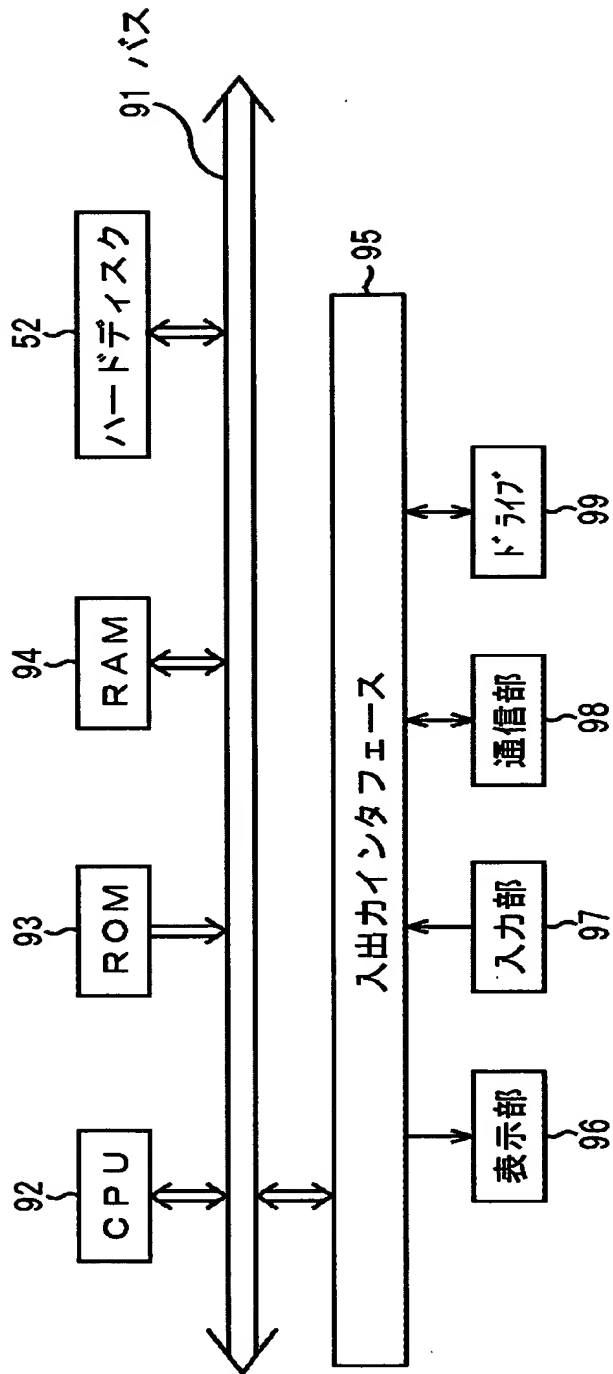
【図 7】



【図 8】



【図 9】



パーソナルコンピュータ 51

【書類名】 要約書

【要約】

【課題】 蓄積されているデータが改竄され、不正に利用されるのを防止する。

【解決手段】 不揮発性メモリ 2 3－1 からハードディスク 1 5 に曲を移動するとき、アプリケーションは、不揮発性メモリ 2 3－1 の media defect list の 0 番目の defect block に記憶されている変数 seq 1 を、新たな値 seq 2 に更新する。アプリケーションは、不揮発性メモリ 2 3－1 のデータ部に記憶されている音楽データを暗号化している暗号鍵と、変数 seq# を含む重要情報とから MAC 値（ハッシュ値）を演算し、その値と、ヘッダ部に記憶されている MAC 値とを比較し、両者が一致しなければ、音楽データの再生を禁止する。

【選択図】 図 7

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社